International Journal of Computer Science Engineering
and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 4, Issue 4, Jun 2014, 93-98
© TJPRC Pvt. Ltd.

IDS (INTRUSION DETECTION SYSTEM) FOR MULTITIER WEB APPLICATION

N. A. PAWAR & Y. C. KULKARNI
B.V.D.U. College of Engineering, Pune, Maharashtra, India

ABSTRACT

Intrusion Detection System plays major role in computer security. This paper is describes Different types of attacks occurred to computer system and preventions that are used to avoid all these attacks. In this paper we do not describe details of existing intrusion detection system. Instead, we focus on detection and prevention of attacks. This paper make introduction of IDS for multitier web application.

KEYWORDS: False Positive, Intrusion Detection System, Signature, Vulnerabilities

INTRODUCTION

In everyday life information Systems and Networks are suffer from attacks. By using Vulnerability information security can be cracked. Firewalls are can be used to prevent unauthorized access into our network. Intrusion Detection System support information system to tackle the attacks. IDS can made this by gathering and analyzing information [1].

Following are Three Main Components to the Intrusion Detection System

Network Intrusion Detection System (NIDS): When traffic can be passed on the entire network NIDS performs an analysis on them. When the traffic can be passed on the subnets if the attack is identified Then it send alert to the administrator. E.g. firewall [2].

Network Node Intrusion Detection System (NNIDS): When the traffic can be passed from the network to a host then it perform analysis. In NNIDS traffic is controlled on the single host. e.g.installing it on a VPN device.

Host Intrusion Detection System (HIDS): In this IDS system we can match existing snap with previous snapshot. The administrator investigate if the critical system files were modified or deleted, e.g. in mission critical machines do not change their configuration.

MODULES IN PROPOSED PAPER

- **Static Website**

In static website we can allow user to access some images and files from web server generating static requests. In static website we use upload and download files, folders and different images.

- **Dynamic Website**

In dynamic website we can allow site visitors to read, post, and comment on articles. Dynamic website like blogs requires regular updating of database. This website will accept web request and generate all types of mappings except no matched request described in double guard system.

- **How Attack Occur**

In this we are showing how attacker can attack to our system and harm our system. Attacks like sql injection, privilege escalation, session hijacking, direct db attack in previous system and we add our own new searched attacks like Brute force attack and Input validation attack.

- **Prevent Website from Attack**

In this we are showing how our system can be prevent from those types of attack. this is the key goal of our paper.

Architecture

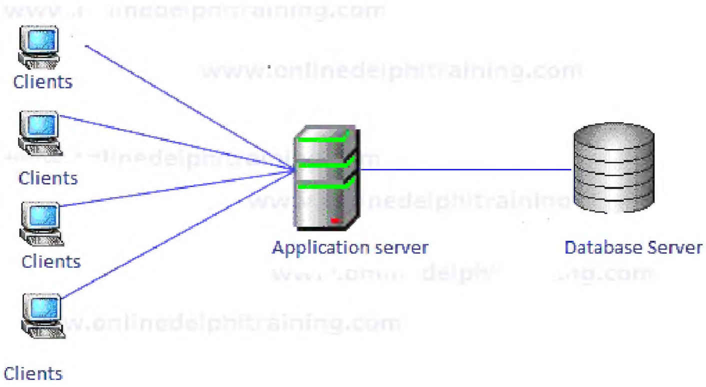

Figure 1: Multitier Web Architecture

Figure 1 illustrates the classic 3-tier model. At the database side, there is no proper transaction between client and web server. It is very hard to tell which transaction corresponds to which client request. The communication between the web server and the database server is not distinguished and to understand the relationships among them is very difficult.

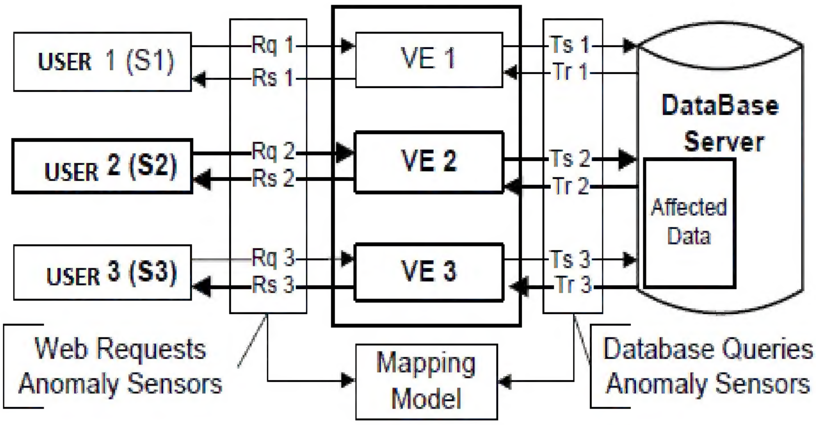

Figure 2: Web Server Instances Running in a Container

Figure 2 shows communication between sessions and database of its respective session. In this Figure 2. Only user 2 data in database can be affected. In this Figure Client and server separated by session

Mapping and Patterns

Different web applications posses different characteristics. There are two types of websites present one is static while another is dynamic. All content present in static websites is static, that content can be managed by CMS

(Content Management System). In static website we always get the same information while clicking on the same link. In Dynamic Websites users are allowed to update the data. It becomes difficult for IDS to prevent attacks in Dynamic websites because of its changing variables. To clarify the mapping patterns which are used in this paper, suppose, session i has set of requests, which is Ri, with a set of queries, which is Qi. Consider training phase has number of sessions are N, then total web requests are REQ, adding set of sql queries are SQL for all sessions.rm denote number of request in Ri, where i=1,2,.........N

Following Mapping Patterns are Used in our Paper

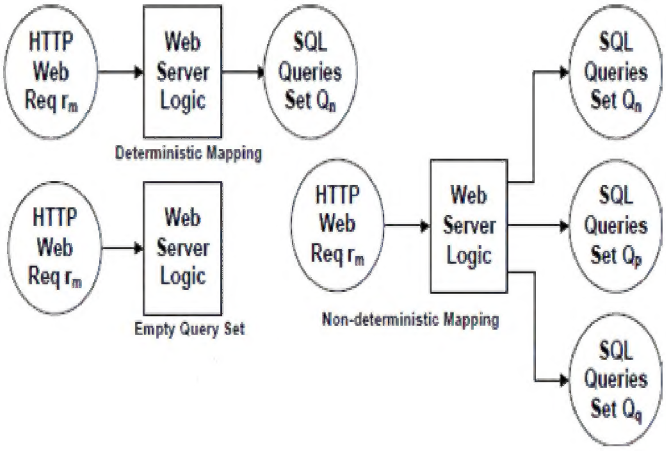

Figure 3: Overall Representation of Mapping Patterns

- **Deterministic Mapping**

This is common and exact matched pattern. All traffic with The SQL queries set Qn contain web request rm. rm ! Qn (Qn 6= ;) is mapping pattern. For any session for the absence of query set Qn and web request rm it creates intrusion.

- **Empty Query Set**

The SQL query set may be the empty set for special situations. This indicates that the web request not only causes but also generates any database queries. For example, web request for retrieving an image GIF file.This type of mapping is indicated as a rm!;.

- **Non-Deterministic Mapping**

There are different SQL query sets for same web request are based on input parameters. After that it creates pool of query sets. Query in the query pool each time match with same web request. rm!Qi is the mapping pattern of this type of mapping.e.g. dynamic websites.

METHODOLOGY

Exsisting Attacks

- **Privilage Escalation**

In this attack hacker find drawback of system & hack administrator rights. Website is used for both regular users and administrators. Attacker logs into system as a normal user and upgrade his privileges.Attacker in this attack triggers admin queries for obtaining administrator data.

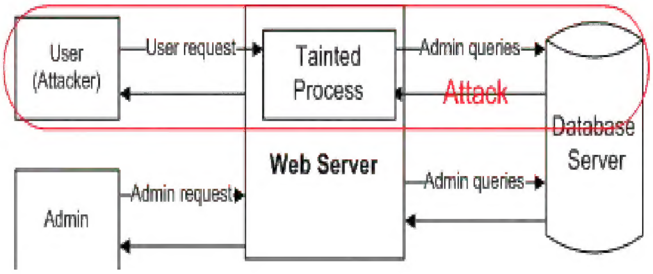

Figure 1: Privilege Escalation Attack

- **Hijack Future Session Attack**

In this attack history of another user can be hacked by hacker. This type of attacks is occured at the web server side. An attacker take control of the web server and hijacks all the data related to user.

By hijacking another user data attacker send unwanted replies and ignore the request of user. A session hijacking attack can be further classified as a Spoofing/Man-in-the-Middle attack, an Exfiltration Attack, a Denial-of-Service/Packet Drop attack, or a Replay attack.

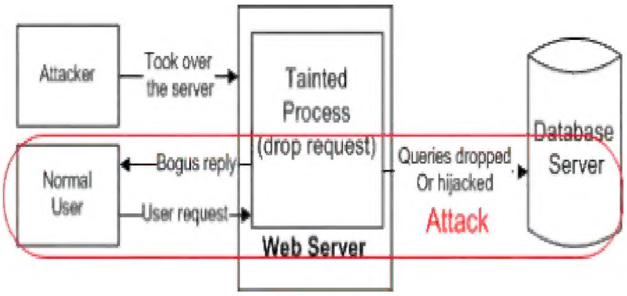

Figure 2: Hijack Future Session Attack

- **Injection Attack**

In this attack hacker calls or inject sql query. Attacker can type another user password & email id & attack another user account. Attacks such as SQL injection do not require help of the web server. To attack on the web server attackers can use existing vulnerabilities in the web server and inject the data or string content that contains the destroyed user information.

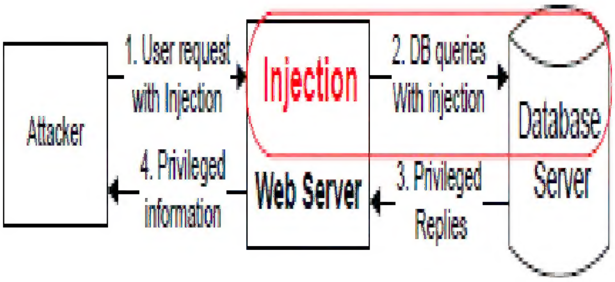

Figure 3: Injection Attack

- **Direct DB Attack**

In this attack database does not find out apostrophe in any sentence & sentence after this can be consider as malicious data by database. In direct db attack attacker can submitting queries directly to the web server without sending web request for it

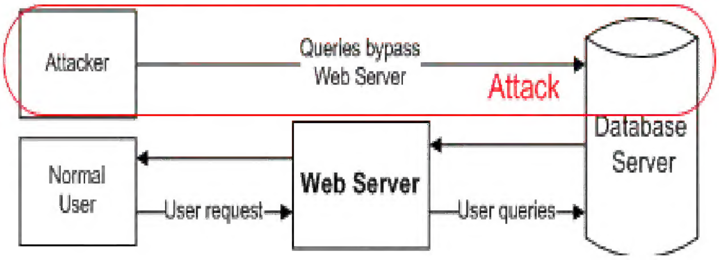

Figure 4: Direct Database Attack

Pruposed Attacks

- **Input Validation Attack**

In this attack hacker disable javascript, so that invalid validation can be accepted by login page. The origin of most attacks is input validation attack.In this attack all the inputs thats received to the web server should be considered as valid.all these inputs are data types,data ranges,buffer sizes and metacharacters. Javascript can be bypassed in this attack.To avoid this attack we notify the attacker that without enabling javascript he/she cannot login to that page .

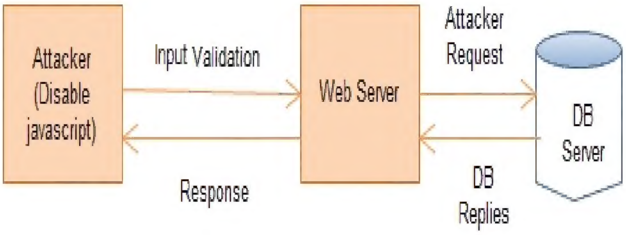

Figure 1: Input Validation Attack

- **Brute Force Attack**

Continuous trying list of different passwords,words or letters do not decrypt any information. In brute force attack to gain access of account of other user attacker continueously used guessed password or words.A brute force attack involves trying every key combination to find the correct password that will hack an account of another user.

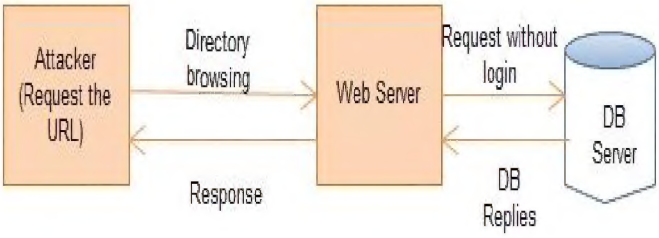

Figure 2: Brute Force Attack

Prevention Measures to Avoid Following Attacks

- **Privilage Escalation**

To avoid this attack user do not known to hacker whether he has to login either user or admin.

- **Session Hijacking**

To avoid this attack user cannot get history .If user check backlink, if backlink is not present Then redirect to login page.

- **Sql Injection**

To avoid to hack the query we can stored our database on backend i.e. in the form of database, in the form of stored procedure.

- **Direct Database**

To avoid this attack user can use double apostrophic so that in database it can get it directly.

- **Input Validation**

To avoid this attack we put message there without enabling javascript we cannot get that data

- **Brute Force**

To avoid this attack after certain fixed tried by hacker , account can be blocked for certain period.

CONCLUSIONS

We presented an intrusion detection system that builds models for multi-tiered web applications from both front-end web (HTTP) requests and back-end database (SQL) queries. We tried to model static and dynamic web requests with the back-end file system and database queries. We show that attacks that are occurred at static as well as dynamic websites. Instead of using different code for static as well as dynamic websites we use same IDS for both of them. We use IIS instead of Open VZ framework that can be used in previous paper. By using minimal false positive Double Guard detects attacks.

ACKNOWLEDGMENTS

The authors would like thanks to the publishers, researchers for making their resources available and teachers for their guidance. We would also thank the college authority for providing the required infrastructure and support. Finally we would like to give a heart fully gratitude to friends and family members.

REFERENCES

1. Intrusion Detection and Response - Lawrence Livermore National Laboratory Sandia National Laboratories, December, 1996 URL: http://all.net/journal/ntb/ids.html
2. Intrusion Detection FAQ , SANS Institute http://www.sans.org/newlook/resources/IDFAQ/ID_FAQ.htm.

AUTHOR DETAILS

Ms. Nayana. A. Pawar received a B.E. (Comp. and Sci.) in 2009 from Shivaji University. I am pursuing a Master Degree in Information Technology from Deemed University B.V.D.U.C.O.E. Pune 46. My interest and research area is Computer security.